	Montana Operations Manual ***Policy***	Category	**Information Technology, Infrastructure**
		Effective Date	**No Date Set**
		Last Revised	**Not Approved Yet**
Issuing Authority	**Department of Administration** **State Information Technology Services Division**		

POL-System Development Life Cycle (SDLC) Policy

I. Purpose

The Montana Information Technology Act (MITA), Sections 2-17-504 et seq., MCA, assigns the responsibility of establishing and enforcing statewide IT policies and standards to the Department of Administration (DOA) 2-17-512 (1)(e), MCA. Rule 2.12, Administrative Rules of Montana has been adopted to interpret and implement MITA. The purpose of this Policy is to implement the POL-System Development Life Cycle Policy for defining actions to fulfill the responsibility.

II. Scope

This Policy applies to the State Chief Information Officer (CIO) as required under Sections 2-17-511and 2-17-512(1)(e), MCA, and to executive branch agencies, as provided in Section 2-17-505(4)(a), MCA, excluding the university system, Section 2-17-516(2), MCA. This policy does not apply to the national guard or the criminal justice information network, Sections 2-17-516 and 2-17-546, MCA.

III. Policy Statement

This enterprise policy has been developed for the state's information systems based on MITA. This policy is in cooperation with federal and local governments with the objective of providing seamless access to information and services to the greatest degree possible. Section 2-17-505 (4).

This policy also describes the requirements for developing and/or implementing new software and systems for the State of Montana and to ensure that all development work is compliant as it related to any and all regulatory, statutory, federal, and/or state guidelines.

IV. Roles and Responsibilities

Roles and responsibilities are required by this policy and defined in accordance with POL-Information Security Policy - Appendix B (Security Roles and Responsibilities).

V. Requirements

State agencies are responsible for developing, maintaining, and participating in a Systems Development Life Cycle (SDLC) for State system development/implementation projects.

The following shall apply for all State information systems:

1. At a minimum, a system development life cycle shall include these phases:
   a. **Initiation.** The need for a system is expressed and the system purpose and high-level requirements are documented.
   b. **Acquisition/Development.** The system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles.
   c. **Implementation/Assessment**. After initial system testing, the system is installed or fielded.
   ~~c.~~ Repeat b. and c. as necessary.
   d. **Operations/Maintenance**. The system performs the work for which it was developed.
   e. **Disposal.** The system is disposed of once the transition to a new computer system is completed, or the data that must be maintained for retention purposes is stored appropriately for records retention.

   This methodology ensures that the system will be adequately documented and tested before it is used in conjunction with critical and/or sensitive agency information.
2. All development work shall exhibit a separation between production, development, and test environments, and at a minimum have at least a defined separation between the development/test and production environments unless prohibited by licensing restrictions or an exception is made. These separation distinctions allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.

Formatted: Font: Not Bold

Formatted: Indent: Left: 1", No bullets or numbering

3. ~~Where these separation distinctions in environments have been established, d~~Development~~,~~ and QA/test staff may only be permitted to have read-only access to production systems unless ~~absolutely~~ required by their respective job duties/descriptions.

4. All application/program ~~access~~entry points ~~paths~~ utilized in development or testing~~,~~ other than the formal user access paths (backdoors), must be deleted or disabled before software is moved into production.

5. Documentation must be kept and updated during all phases of development from the initiation phase through implementation and ongoing maintenance phases. Additionally, the creation of security documents, i.e. Risk Assessment, Disaster Recovery, or an Information Security ~~Risk Mitigation~~ Plan must be completed before systems move into production or the disposition phase.

6. All software and web applications that create, manage, use, or transmit Level ~~1~~3 information, as defined by the data classification policy, must be developed and maintained solely by State of Montana personnel. Other development work involving Level ~~2~~1 and Level ~~3~~2 information may be done outside of State IT provided the State Systems Development Life Cycle (SDLC) Standards are followed. Determining classification level should be done according to an assessment of the need for confidentiality of the information.

7. Agencies must maintain adequate funding for infrastructure and maintenance costs for all systems that they own. If an agency decides to continue with a system after the decision is made to decommission the system from an enterprise perspective, they must maintain funding for extended maintenance and security updates. The adequate funding necessity includes the requirement to purchase extended maintenance for software and hardware that is beyond the vendor's defined lifecycle. This is often referred to as extended support. Systems must maintain a minimum of current or one version back on all software.

8. Review of systems must be completed on an annual basis to determine whether they should be transferred, have become obsolete, or are no longer usable. ~~If it is determined that a system is being used less than 50% of the time, by less than 50% of customers from highest utilization, or has lost more than 50% of its customers at highest utilization, then a~~An official termination date of the system should be established if the agency determines that the system has minimal business value or usefulness. This is determined through a baseline ROI evaluation or business case. Decommissioning of a system should be completed over the least amount of time possible.~~a period of time not to exceed four years.~~

9. Disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. A disposition review must be conducted to ensure that a system/application has been completely and appropriately disposed, thereby ending the lifecycle of the IT project. If data is involved, a data migration/archival or disposal path should be established.

   The phase-end review shall be conducted again within and after six months of the retirement of the system. A Disposition Review Report documents the lessons learned from the shutdown and archiving of the terminated system.

   ~~The following chart and references have been developed by NIST 800-160 to outline the SDLC process and should be utilized for this purpose.~~

VI. Definitions

Refer to the GDE-Statewide Glossary: Information Systems Policies and Standards for a list of local definitions

VII. Enforcement

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards must be prioritized and acted upon based upon impact and need.

Enforcement for statewide polices and standards developed in accordance with this policy must be defined in each policy, standard or procedure. Policies and standards not developed in accordance with this policy may not be approved as statewide IT policies or standards.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy may be found in the MOM Policy System (search for: 261). When considering formal disciplinary action, management shall consult with their assigned Human Resource Specialist before taking action.

VIII. References

A. Legislation

- Section 2-17-511, MCA
- Section 2-17-512, MCA
- Section 2-17-516, MCA

- Section 2-17-546, MCA
- Montana Information Technology Act (MITA), Sections 2-17-504 et seq., MCA

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- Statewide Policy: POL-Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Policy: POL-Information Security Policy - Appendix A (Baseline Security Controls)
- Statewide Policy: POL-Information Security Policy - Appendix B (Security Roles and Responsibilities)
- SITSD Procedure: IT Policies, Standards, Procedures and White Papers
- Rule 2.12, Administrative Rules of Montana
- State of Montana Office of the Governor Executive Order No. 09-2016
- NIST Policy SP 800-64 Rev 2 Security Considerations in the System Development Life Cycle

C. Standards, Guidelines